

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The 18 items listed in attachment A, all securely stored
at the FBI St. Louis Office at 2222 Market Street in St.
Louis, MO 63103, Within the Eastern District of Missouri.

Case No. 4:23-MJ-9108 RHH

SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

Title 18, United States Code, Sections 2251 and 2252A - production, receipt, distribution, and possession of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

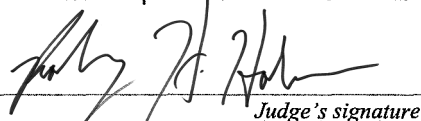
I state under the penalty of perjury that the foregoing is true and correct.


Applicant's signature

Brian VanderWoude, Special Agent
Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41.

Date: 06/30/2023


Judge's signature

City and state: St. Louis, MO

Honorable Rodney H. Holmes, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
The 18 items listed in attachment A, all
securely stored at the FBI St. Louis Office at
2222 Market Street in St. Louis, MO 63103,
Within the Eastern District of Missouri.

No. 4:23-MJ-9108 RHH

SIGNED AND SUBMITTED TO THE
COURT FOR FILING BY RELIABLE
ELECTRONIC MEANS

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A SEARCH WARRANT**

I, Brian VanderWoude, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – electronic devices – described in Attachment A, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since August of 2021. I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of the internet, computer devices and cellular telephone to commit crimes such as violations of Title 18, United States Code, Sections 2251 and 2252A, which proscribe sexual exploitation of minors. As an FBI Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251 and 2252A, (the “SUBJECT OFFENSES”) have been committed by **RUSSELL PIRKEY**, or other persons known and unknown. Sections 2251 and 2252A criminalize, among other things, the production, receipt, distribution, and possession of child pornography. There is also probable cause to search the devices described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

5. The property to be searched is:

1B1. SanDisk 8 GB Micro SD Card

1B2. SanDisk 16 GB Micro SD Card with SanDisk Adapter

1B3. LG SD Card labeled movies

1B4. Transcend Micro SD Card 64 GB, Model B08550

1B5. SanDisk 8GB Micro SD Card

1B6. 2 GB Micro SD Card with Plastic Case

1B7. SanDisk Pixtor 32GB Micro SD Card

1B8. Samsung Evo 16 Micro SD Card with Adapter

1B9. SanDisk 2GB Micro SD Card with plastic case

1B10. SanDisk 1 GB Micro SD Card

1B11. Blue Lexar SD Card 512 MB

1B12. Samsung Cell Phone, IMEI 352625665091664

1B13. Pink Kocaso Tablet, Model M752H

1B14. Gray LG Smart Phone

1B15. Black Samsung Cell Phone with cracked screen

1B17. PNY 2GB SD Card

1B18. SanDisk 4GB Micro SD Card

1B19. Black Micro USB with black grip

(hereinafter “the Devices”).

The Devices are currently located at the FBI St. Louis office, located at 2222 Market Street in St. Louis, MO, within the Eastern District of Missouri.

6. The applied-for warrant would authorize the forensic examination of the devices for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. The term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator, or other similar device. 18 USC § 1030(e).

- b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.
- c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras

also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- d. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna

can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- f. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- h. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- i. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game consoles and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- j. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- k. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

- l. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- m. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- n. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.
 - o. The term “minor” means any individual under the age of 18 years. 18 USC § 2256(1).
 - p. Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person. 18 USC § 2256(2)(A).
 - q. Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).
 - r. Child pornography means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) or (C).
8. Based on my training, experience, and research, I know that some of the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS, PDA, computer, as well as a storage device for records, documents, materials and

electronic data, and a means of access to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, contraband as well as evidence that reveals or suggests who possessed or used the Devices, how the Devices were used and where the Devices were possessed.

PROBABLE CAUSE

9. On April 8, 2023, Brookfield Police Department (BPD), responded to 217 E. Clayton Street in Brookfield, Missouri to a report of a possible sexual assault. Upon arrival, the reporting officer made contact with a female C.L. who stated she was informed by her son that a juvenile female, R.M., 10 years of age, was dating a 52-year-old man by the name of Jason. C.L. then went to R.M.'s home, 217 E. Clayton Street, to inform R.M.'s parents that R.M. was dating a 52-year-old man. C.L. was informed by Eric Miller, a resident of 217 E. Clayton Street, that R.M. was currently in the residence's garage with Jason. C.L. went to the garage and retrieved R.M., who appeared to be in emotional distress, and brought R.M. to wait in C.L.'s vehicle until law enforcement arrived.

10. The responding BPD officer made contact with R.M. inside C.L.'s vehicle. R.M. stated, "he kept on touching my thigh, and I didn't like it." BPD officers spoke with Eric Miller who informed officers that Jason was inside the home. BPD officers requested that Eric Miller retrieve Jason from inside the residence. Jason exited the home and was detained by BPD. Jason informed officers that his true name was Russell PIRKEY (hereinafter referred to as PIRKEY). R.M. identified PIRKEY as the man who touched her thigh and stated that his name was "Russ".

11. R.M. informed BPD officers that she was alone with PIRKEY in the garage at 217 E. Clayton Street. BPD located R.M.'s cell phone, 1B12 - Samsung Cell Phone IMEI:

352625665091664, outside of 217 E. Clayton Street and seized the phone as evidence. R.M. was transported to BPD to wait for her mother J.M. to arrive.

12. Upon arrival at BPD, J.M. provided consent for officers to review the contents of R.M.'s cell phone. A consent to search computer/electronic equipment form was completed and signed by J.M. During review of the R.M.'s cell phone, BPD observed a video that was a screen recording from TikTok, which contained a message from the account "Russ" to R.M.'s account stating that he was "hard" and included several explicit conversations. While in custody at BPD, PIRKEY confirmed that he had a cell phone and tablet located in the garage of residence 217 E. Clayton Street Brookfield, MO. PIRKEY denied consent to BPD to review the contents of the cell phone and tablet.

13. On April 8, 2023, BPD applied for and obtained a search warrant in the Circuit Court of Linn County, Missouri for the residence of 217 E. Clayton Street Brookfield. The search warrant included any electronic device including: cellphones, tablets, USB drives, laptop computers, etc. that could be used in the communication of sexually explicit images and messages to a minor. During the execution of the search warrant on April 8, 2023, the following items were seized and placed into evidence at BPD; 1B13 - pink kocaso tablet model M752H, 1B14 - gray LG smart phone, 1B15 - black Samsung smartphone with cracked screen.

14. On April 12, 2023, a forensic interview of R.M. was conducted by the North Central Missouri Children's Advocacy Center in Trenton, Missouri. During the interview R.M. disclosed that PIRKEY had touched her on multiple occasions. R.M. stated that PIRKEY would apply lotion to his hands prior to digitally manipulating R.M.'s genitals. R.M. described the lotion as a green and white bottle located next to PIRKEY's bed. R.M. continued to disclose that PIRKEY forced

her to watch pornography on his phone, which included videos of men, women, and some children. R.M. stated that while watching pornography, PIRKEY would insert his finger into R.M.'s vagina.

15. On April 19, 2023, a second search warrant was issued for the property of 217 E. Clayton Street to include vehicles, detached garages, any locked boxes, clothing, and bedding. The search detailed the seizure of lubrication, pornographic material, and any electronic devices that could be used to view pornographic material. During the execution of the search warrant the evidence items identified as 1B1-1B11 and 1B17-1B19, as described in paragraph 5 above, were seized and placed into evidence at BPD.

16. All evidence items listed in Attachment A were transported to Kirksville Regional Computer Crime Unit (KRCCU) located in Kirksville, Missouri to complete a forensic examination.

17. On June 9, 2023, your affiant collected evidence items 1B1 - 1B15 and 1B17 - 1B19 from KRCCU and transported them to the FBI St. Louis Evidence Control Room.

18. Your Affiant believes that there is probable cause that evidence of PIRKEY's violations of Title 18, United States Code, Sections 2251 and 2252A are contained on the Devices listed in attachment A.

19. In my training and experience, I know that the devices have been stored at the FBI in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. In my training and experience, I know that cellular phones ("smartphones"), contain software and hardware that are the same, if not more sophisticated, than a typical home computer.

The term “computer,” “hard drive,” and “computer media,” as used in this affidavit, also refers to cellular “smart” phones.

21. I also know that “smartphones” often allow for cloud-based storage, and many users back up their phones on their home computers. Information contained in a cell phone that is connected to a desktop, laptop computer, or the cloud, can easily transfer onto other media.

22. A computer’s ability to store images in digital form makes a computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

23. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

24. Collectors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, iCloud, and Hotmail, and social media applications such as Kik and Snapchat among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user’s computer, even if the user is accessing the information on their cellular “smart phone.” Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer in most cases.

25. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be

intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

26. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

27. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

28. In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. Sections 2251 and 2252A, and should all be seized as such.

29. Affiant knows from training and experience that even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner. Specifically, when a

user deletes a file, it goes into a “trash” folder. When the user directs the computer to “empty” the trash folder the contents of the folder, including the deleted file, disappear. However, the file has not left the computer and under normal circumstances, is recoverable by computer experts until it’s overwritten because there is no longer unused space in the computer’s hard drive. How soon a file will be overwritten depends on a number of factors: whether the user is computer savvy and has installed a program that accelerates the normal overwriting of deleted data, how often new files are saved to his hard drive, the capacity of the hard drive, and how the computer’s file system allocates new files. Trained certified computer forensic examiners routinely extract incriminating deleted files from hard drives, usually without difficulty.

30. Since a deleted file is not overwritten all at once, it may be possible to reconstruct it from the bits of data composing it (called “slack data”), which are still retrievable because they have not yet been overwritten even if overwriting has begun. Before a file is deleted, the file system marks it as unavailable to be overwritten. Once it is deleted, its data are no longer protected against being overwritten, but the file system won’t necessarily overwrite it all at once, and if it’s only partially overwritten computer experts can recover the portion of the data that has not been overwritten, or at least can match it to images they obtained from, for example, a website, to verify that the images were once in the computer’s hard drive and thus had been possessed. Although a savvy computer user can direct his computer to ensure quick (even instantaneous) overwriting, the default settings on standard operating systems do not do this.

31. It is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which specific expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it. No matter which method is used, the data analysis protocols that will be utilized are exacting scientific procedures, designed to protect the

integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Upon approval and execution of the search warrant, in appropriate circumstances, a forensic image (also known as a bit-stream image), which is an exact physical copy of the seized electronic evidence, will be created so that their contents could be examined at a field office or computer laboratory and/or other locations following completion of the on-site search.

32. The search of computers, hard drives, and other seized electronic media will include a complete search of the entire piece of seized electronic evidence. A computer forensic examiner cannot rely on the name of a file to exclude or confirm the existence of child pornography within that file. Individuals will intentionally mislabel directory structures, folder names, and filenames to hide the presence of child pornography. In other cases, an individual may not attempt to hide the child pornography but utilize a unique naming convention or organizational methodology which may inadvertently hide the presence of child pornography. In order to perform a comprehensive forensic examination, a computer forensic examiner must conduct an all-inclusive examination of every bit (or binary digit) on the particular electronic storage device.

33. Moreover, hard drives and other pieces of electronic media have unallocated space which might contain deleted files, records, relevant e-mails, other communications, and search terms related to the possession, receipt, and distribution of child pornography. Thus, without looking at the entirety of the electronic media for evidence related to child pornography, the investigator may not find evidence relevant to the criminal investigation.

SEARCH METHODOLOGY TO BE EMPLOYED


34. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);
- b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

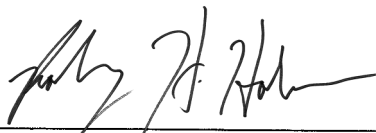
CONCLUSION

35. Based on the foregoing I submit that this affidavit supports probable cause for a warrant to search the devices described in Attachment A and seize the items described in Attachment B.

I state under the penalty of perjury that the foregoing is true and correct.


BRIAN VANDERWOUDE
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 30th day of June 2023.


HONORABLE RODNEY H. HOLMES
United States Magistrate Judge

1B1 - ATTACHMENT A

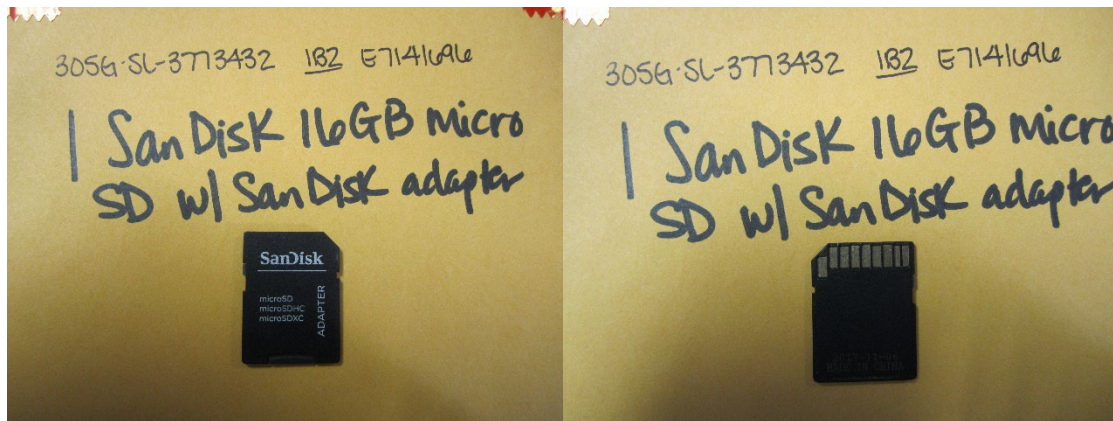
The property to be searched is device **1B1** - (1) SanDisk 8 Micro SD Card, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B1** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B2 - ATTACHMENT A

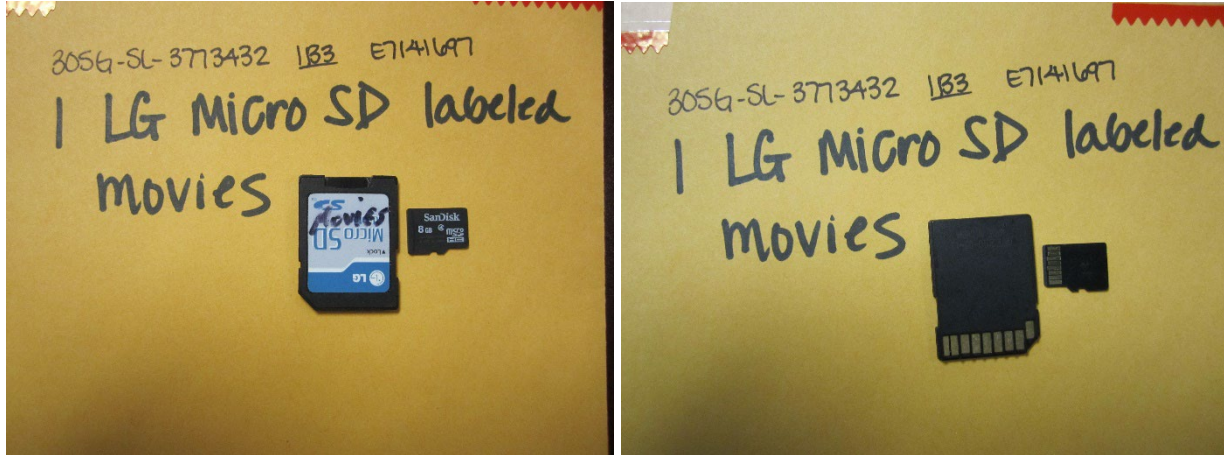
The property to be searched is device **1B2** – (1) SanDisk 16 GB Micro SD Card with SanDisk Adapter, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B2** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B3 - ATTACHMENT A

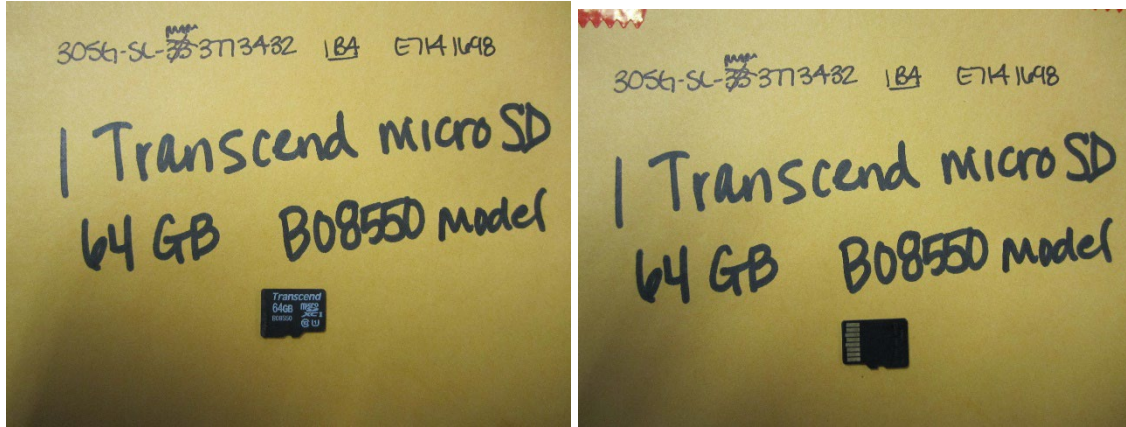
The property to be searched is device **1B3** – (1) LG SD Card labeled movies, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B3** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B4 - ATTACHMENT A

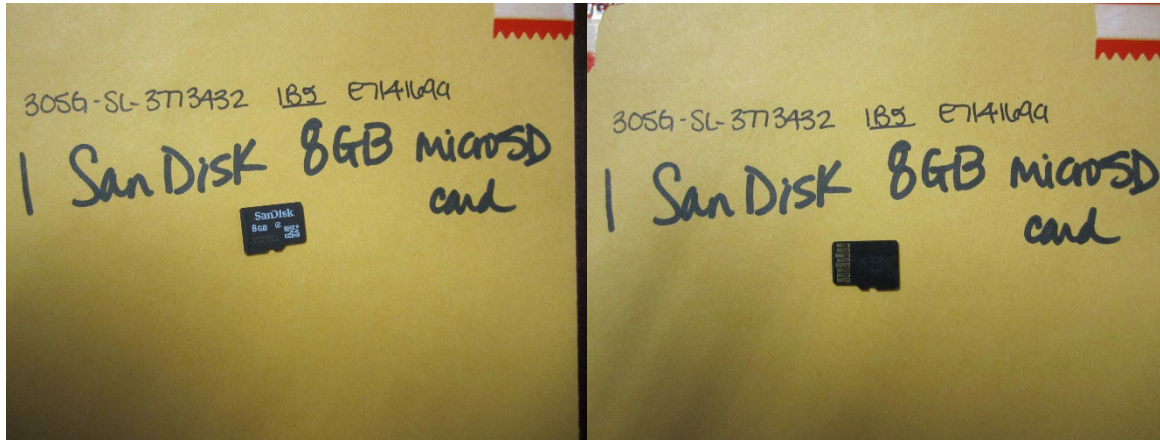
The property to be searched is device **1B4** – (1) Transcend Micro SD Card 64 GB, Model B08550, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B4** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B5 - ATTACHMENT A

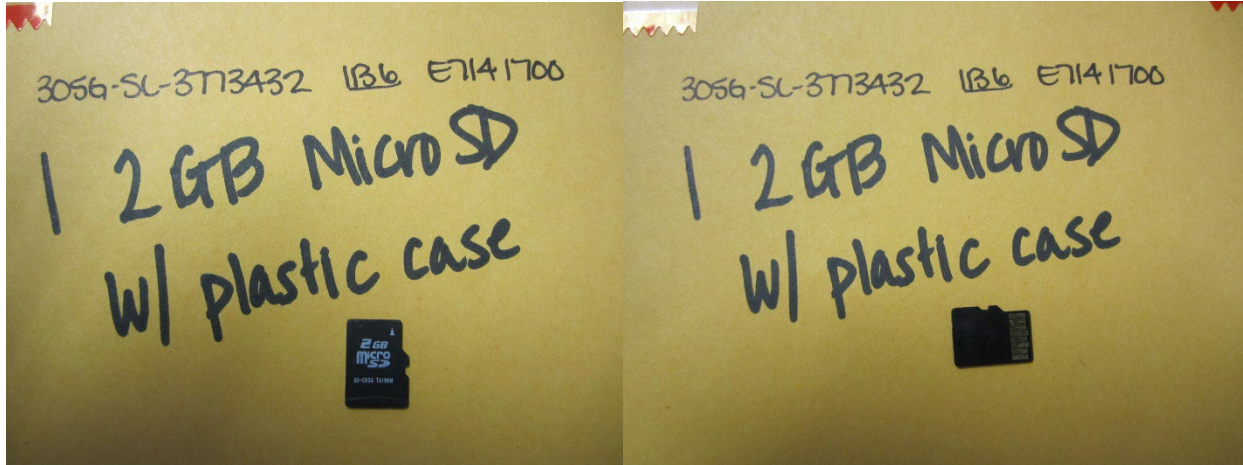
The property to be searched is device **1B5** - (1) SanDisk 8 GB Micro SD Card, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B5** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B6 - ATTACHMENT A

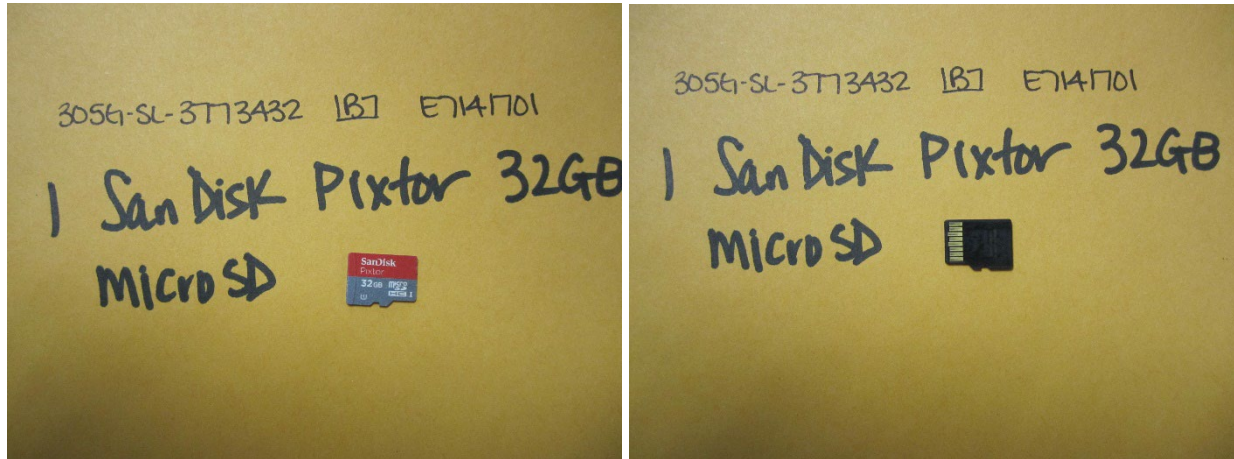
The property to be searched is device **1B6** - (1) 2 GB Micro SD Card with Plastic Case, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B6** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B7 - ATTACHMENT A

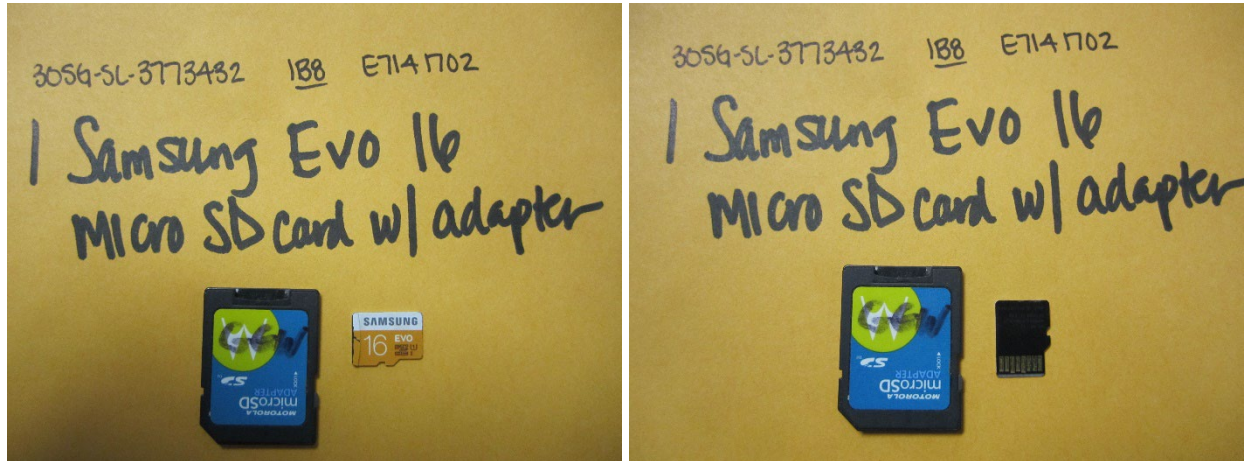
The property to be searched is device **1B7** - (1) SanDisk Pixtor 32GB Micro SD Card, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B7** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B8 - ATTACHMENT A

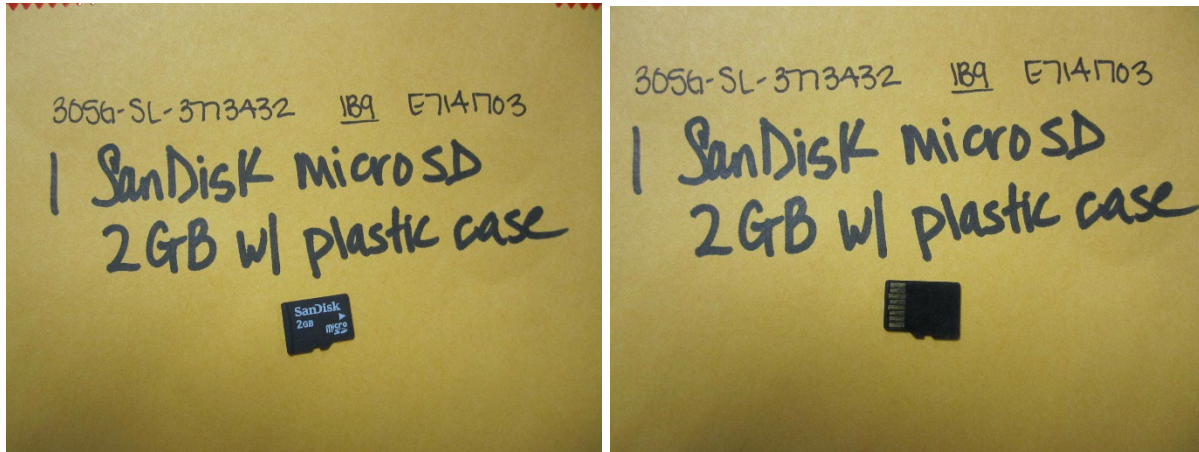
The property to be searched is device **1B8** - (1) Samsung Evo 16 Micro SD Card with Adapter, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B8** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B9 - ATTACHMENT A

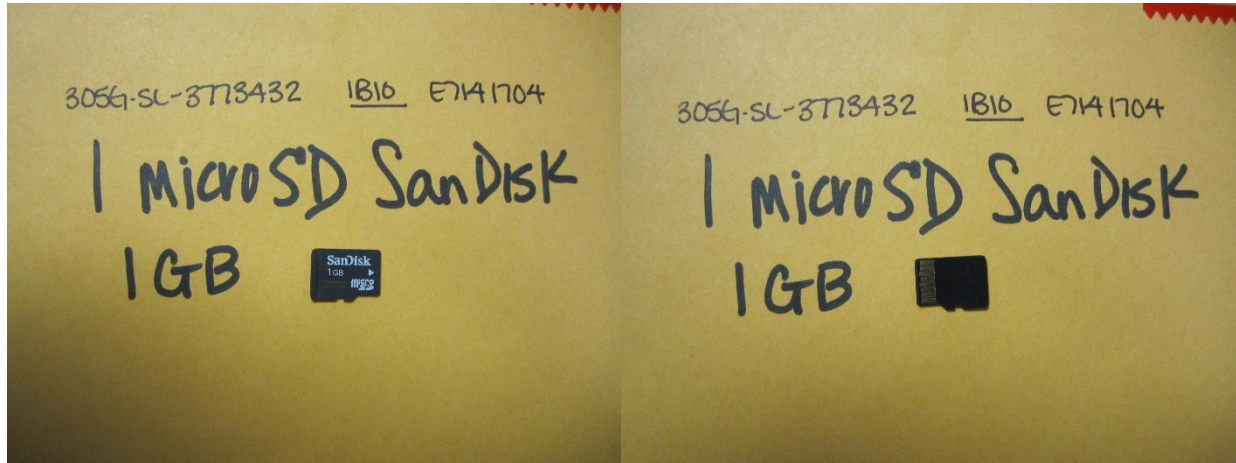
The property to be searched is device **1B9** - (1) SanDisk 2GB Micro SD Card with plastic case, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B9** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B10 - ATTACHMENT A

The property to be searched is device **1B10** - (1) SanDisk 1 GB Micro SD Card, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B10** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B11 - ATTACHMENT A

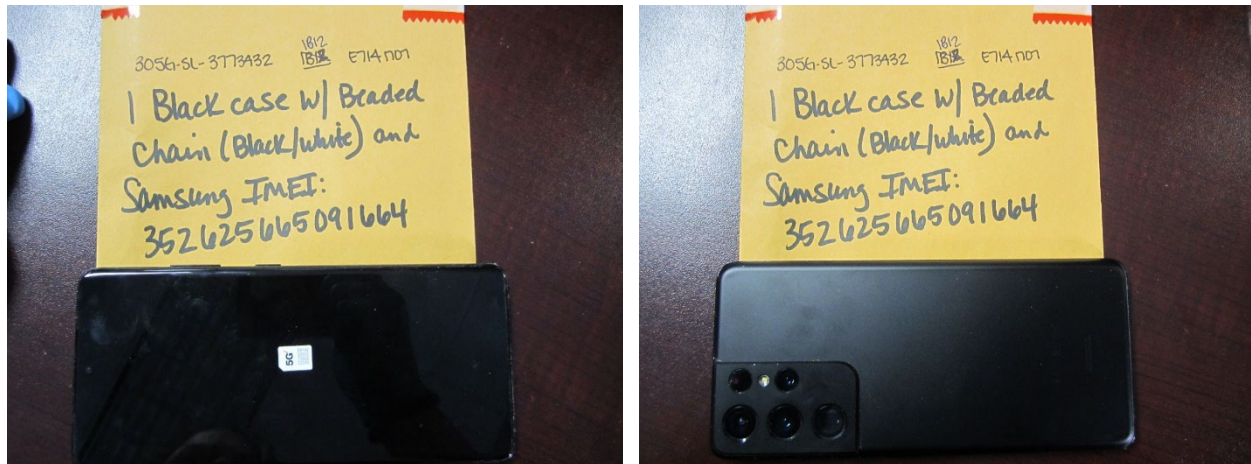
The property to be searched is device **1B11** - (1) Blue Lexar SD Card 512 MB, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B11** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B12 - ATTACHMENT A

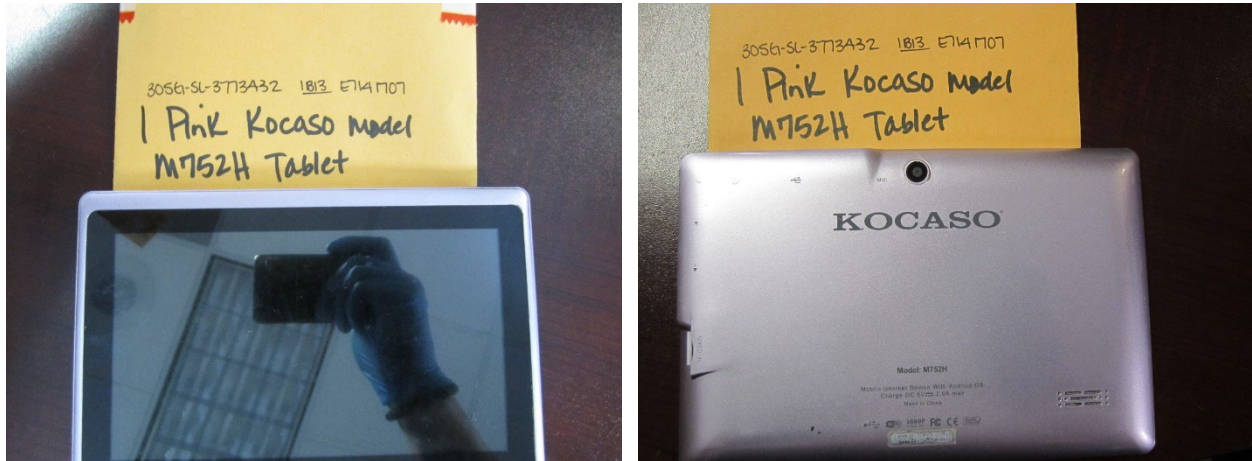
The property to be searched is device **1B12** - (1) Samsung Cell Phone, IMEI 352625665091664, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B12** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B13 - ATTACHMENT A

The property to be searched is device **1B13** - (1) Pink Kocaso Tablet, Model M752H, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B13** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B14 - ATTACHMENT A

The property to be searched is device **1B14** - (1) Gray LG Smart Phone, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B14** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B15 - ATTACHMENT A

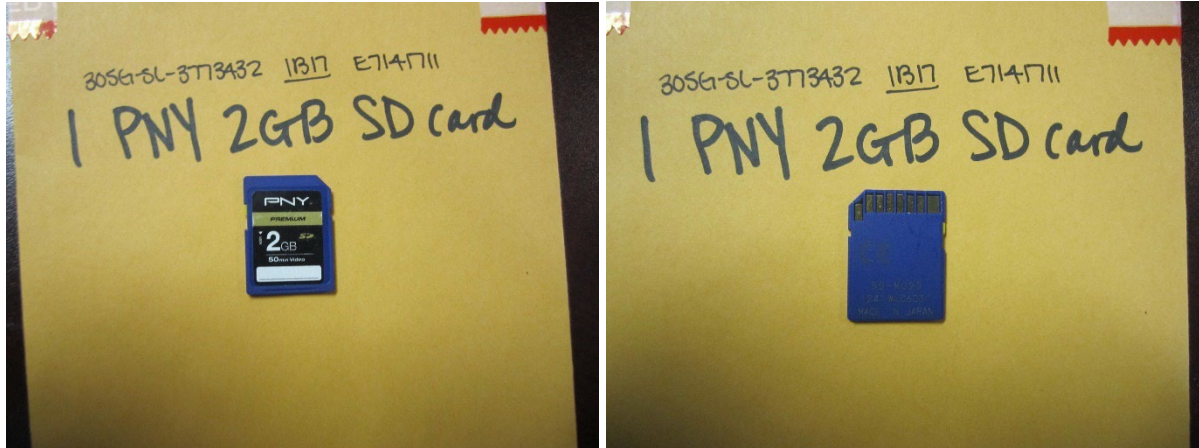
The property to be searched is device **1B15** - (1) Black Samsung Cell Phone with cracked screen, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B15** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B17 - ATTACHMENT A

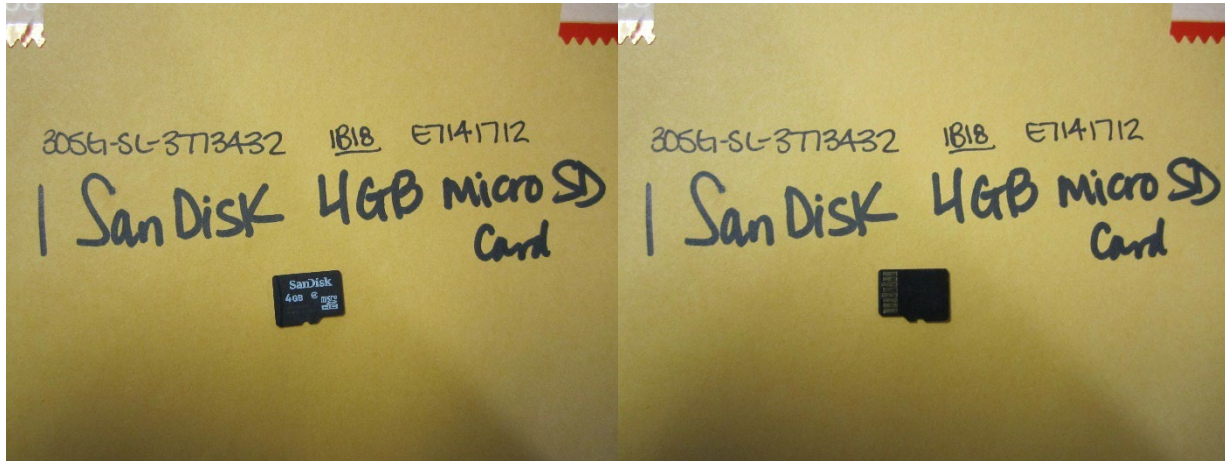
The property to be searched is device **1B17** - (1) PNY 2GB SD Card, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B17** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B18 - ATTACHMENT A

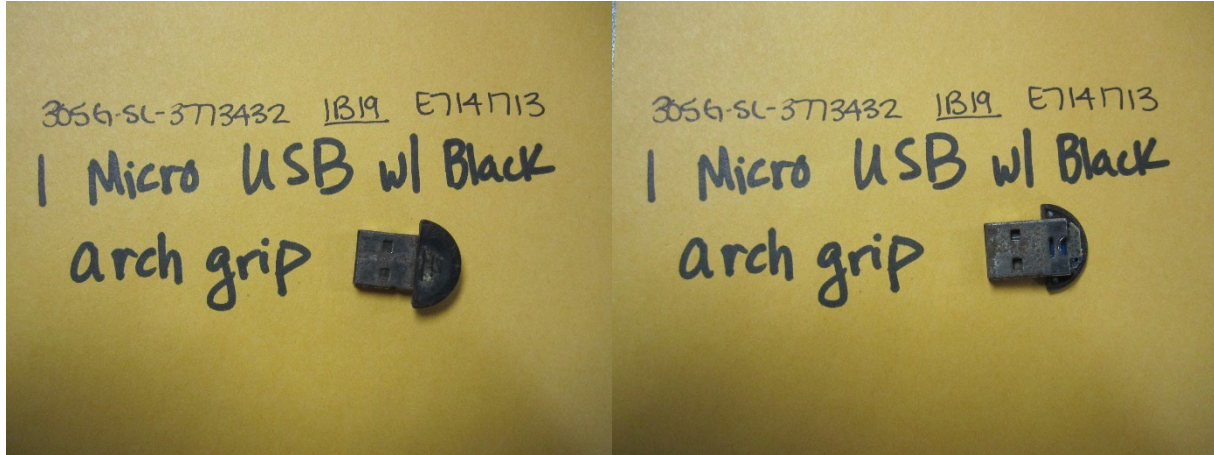
The property to be searched is device **1B18** - (1) SanDisk 4GB Micro SD Card, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B18** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

1B19 - ATTACHMENT A

The property to be searched is device **1B19** - (1) Black Micro USB with black grip, currently located at the St. Louis Office of the FBI, at 2222 Market Street in St. Louis, Missouri, within the Eastern District of Missouri. Device **1B19** is photographed and pictured below:



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following are to be seized from the devices and media listed in Attachment A:

Evidence, instrumentalities and contraband concerning violations of 18 U.S.C. Sections 2251 and 2252A including:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C).
2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
3. Any and all notes, documents, records, correspondence, in any format and medium (including, but not limited to, email messages, chat logs, electronic messages, notes), emails, computer logs, and browser and internet history pertaining the sale of child pornography (or attempt to do so), visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C), sexual exploitation of minors, the grooming of minors indicating of the intent or desire to sexually exploit them, or the enticement of minors to engage in illegal sexual activity.
4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership, possession or use of the Device listed in Attachment A.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted or in contact with Russell PIRKEY by use of: the Device listed in

Attachment A, for the purpose of exchanging child pornography, visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C), sexual exploitation of minors, the grooming of minors indicating of the intent or desire to sexually exploit them, or the enticement of minors to engage in illegal sexual activity.